"To the amendment, p. 2, line 15 thereof, after "functions" delete the period and insert –, while in the former, in a second stage, symmetric encryption can be used to encrypt the intermediate message digest or private key signature value arrived at using the preferred embodiment.—"

Claims: Applicant requests cancellation of claims 63, 64, and 68 of record and substitution of new claims 76-78 as follows, leaving claims 56-62, 65-67, and 69-75 without amendment per the notice filed herewith:

76. A method for signing and verifying electronic data at a server comprising:

    a. an authentication step of creating a collection of records about a plurality of individuals by entering into a data storage medium a collection of any or a combination of any of the following:

        i. personal information about an individual,

        ii. an indicator of the reliability of the identification of the individual who is the subject of a record,

        iii. whether the authentication mode is universal or whether such individual must authenticate to the server computer in order to sign electronic data using the server computer, and

        iv. the authentication credential or plurality of authentication credentials that such individual must present to the server in order to sign;

    b. an access control step of

        i. receiving a request to sign and, unless the authentication mode is universal, an authentication credential or a plurality of authentication credentials from a requestor, and

        ii. comparing the authentication credential or credentials to the information contained in the collection of records to determine if the requestor is an individual who is authorized to sign electronic data using the server;

    c. a presentation step of providing to the server an electronic data set for signature;

d. a transaction identifier step of generating at the server a globally unique
transaction identifier for the electronic data that a requestor intends to sign, which
includes as one input an identifier associated with the requestor's identity;

e. a signature step whereby the server encrypts, as the signature of a signer, each
electronic data set with a unique encryption key, generated from a symmetric
cipher using the globally unique transaction identifier as the character input of a
password for generation of the key;

f. a recording step in which the server generates and stores in a data storage
medium a record of a signature transaction;

g. a verification step whereby

i. an inquiring party seeking to verify the validity of a signature of electronic
data transmits to a server electronic data that is believed to have been
previously signed at a server;

ii. the server determines if a record or a plurality of records corresponding to
the transmitted electronic data exists in the data storage medium of such
records;

iii. the server retrieves a record or plurality of records corresponding to the
electronic data which is presented for verification;

iv. with regard to each such record, the server performs a verification
operation which includes a step of reconstructing a symmetric cipher from
a record of input for a password of a key that was used to create an
encryption key initially, including an identifier of the signer, and applying
such symmetric cipher to decrypt an electronic data set;